Gazi Üniv. Müh. Mim. Fak. Der.
Cilt 25, No 2, 275-283, 2010

J. Fac. Eng. Arch. Gazi Univ.
Vol 25, No 2, 275-283, 2010

FNBDT/SCIP PROTOKOLÜNÜN YEREL ALAN AĞINDA UYGULAMASI VE SINIR DEĞERLERİN TESPİT EDİLMESİ

Orkun DİLLİ, Nursel AKÇAM ve Murat KOYUNCU*
Elektrik-Elektronik Mühendisliği Bölümü, Mühendislik Fakültesi, Gazi Üniversitesi, 06570, Ankara,
*Bilişim Sistemleri Mühendisliği Bölümü, Mühendislik Fakültesi, Atılım Üniversitesi, 06836, Ankara,
odilli@gazi.edu.tr, ynursel@gazi.edu.tr, mkoyuncu@atilim.edu.tr

(Geliş/Received: 20.03.2009 ; Kabul/Accepted: 22.03.2010)

ÖZET

Teknolojideki hızlı değişim her alanda olduğu gibi haberleşme sistemlerinde de yaşanmaktadır. Geliştirilen farklı sistemler veya cihazlar zaman kaybedilmeden kullanıma sunulmaktadır. Söz konusu değişim genelde olumlu olmakla birlikte bazen olumsuz sonuçlara da yol açabilmektedir. Bu olumsuz sonuçlardan bir tanesi, ISDN, PSTN ve IP tabanlı haberleşme cihazlarının birbirleriyle uçtan uca güvenli olarak haberleşme yapamamasıdır. Bu çalışmada, farklı haberleşme ağları üzerinde uçtan uca emniyetli haberleşmenin yapılması amacıyla geliştirilen FNBDT (Future Narrow Band Digital Terminal)/SCIP (Secure Communication Interoperability Protocol) protokolü, emulatörler vasıtasıyla IP ağ üzerinde değişik açılardan test edilmiştir. Bu tür çalışmaların yapılmasının FNBDT/SCIP protokolünün gelişimine katkıda bulunmak açısından büyük önem arz etmekte olduğu ve sunulan çalışmanın bu alanda gerçekleştirilmiş ilk çalışmalardan birisi olması nedeniyle de gelecekte konuyla ilgili yapılacak çalışmalara katkı sağlayacağı düşünülmektedir.

Anahtar Kelimeler: FNBDT, SCIP, uçtan uca güvenli haberleşme.

APPLICATION OF FNBDT/SCIP PROTOCOL ON LOCAL AREA NETWORK AND DETERMINATION OF LIMIT VALUES

ABSTRACT

Fast progress in technologies affects all the domains as well as the communication systems. Different types of systems or devices are developed and given to the services without losing time. Although these progresses, in general, have positive effects sometimes they may cause some problems. One of these problems is that the different terminal devices based on ISDN, PSTN and IP cannot communicate end-to-end with each other in a seamless secure way. In this study, FNBDT (Future Narrow Band Digital Terminal)/SCIP (Secure Communication Interoperability Protocol) protocol, which is developed for end-to-end secure communication of different terminal devices communicating on different networks, is tested from different perspectives using terminal emulator on IP Networks. These types of study have great importance in terms of providing some feedbacks to the development of FNBDT/SCIP and, as one of the initial work on this topic, this study will contribute to the future works in the area.

Keywords: FNBDT, SCIP, end-to-end secure communication.

1. GİRİŞ (INTRODUCTION)

FNBDT/SCIP protokolü, farklı şebekelerde haberleşme yapan cihazların birbirleri ile emniyetli haberleşme ihtiyacından doğmuş bir protokoldür. Protokolle ilgili ilk çalışmalar ABD tarafından FNBDT adı altında başlatılmıştır. Daha sonra, NATO ülkeleri SCIP başlığı altında çalışmaya katılmışlardır.

FNBDT/SCIP'in farklı network ağları üzerinde uygulama alanı bulunmaktadır. Bu çalışmanın IP Ağları üzerinden yapılmak istenmesinin nedenleri;

- IP Ağ uygulamalarının hem taktik hem de stratejik alanda çok yaygın olması,
- Haberleşme alanında IP ağlarının gelecekte daha da yaygın olarak kullanılacak olması,
- FNBDT/SCIP'in IP ağları üzerinden G.711 (64kbps) ve G.729 (8kbps) gibi yüksek bant genişliği tahsisi yapan ses kodeklerini kullanmaksızın, Stanag 4591 Standardına uyumlu 2,4 kbps hızında MELP (Mixed Excitation Linear Prediction) [1-4] ses kodeğini kullanarak az bir bant genişliği tahsisi yapması

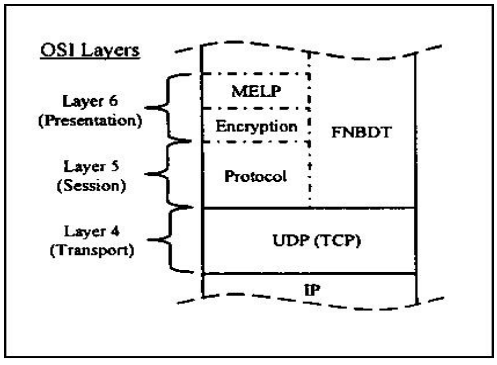
olarak belirtilebilir.

IP dünyasında paket kayıpları fazla miktarlarda olabilmektedir. Fakat gerçek zamanlı uygulamalarda ses paketlerinin kaybolması ses haberleşmesini ciddi ölçüde etkiler. Bu çalışma, IP altyapısında FNBDT/SCIP haberleşme davranışlarının değişik durumlar altında gözlenmesi maksadıyla yapılmıştır. IP ortamında FNBDT/SCIP'in nasıl davranacağı bilinmediğinden birtakım test verilerinin alınması gelecekte FNBDT/SCIP ile ilgili IP ağları üzerinde çıkabilecek olan sorunlara çözüm yolu sağlayacak ve referans olabilecektir. Bu çalışma bu alanda yapılan ilk uygulamanın [5] bütününü içermesi ile dikkat çekmektedir. Bu çalışma ile, çağrı kurma ve farklı modlarda ses ve veri haberleşmesinde çok önemli yeni veriler elde edilmiştir. Bu veriler, bu alanda yeni ve farklı çalışmalar yapacaklara ışık tutacaktır.

2. FNBDT/SCIP SİNYALLEŞMESİ (FNBDT/SCIP SIGNALING)

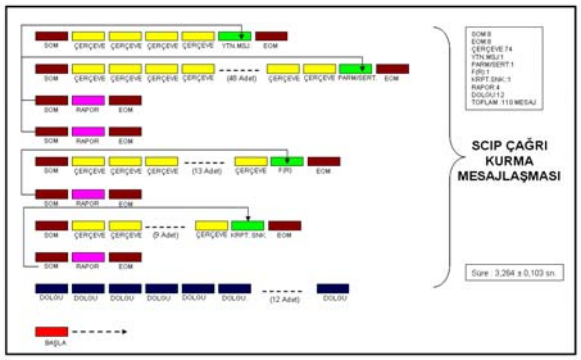
FNBDT, yeni ismiyle SCIP Protokolu, Şekil 1'de görüldüğü gibi UDP protokolü üzerinde çalışır. Kriptolama işlemi Layer 6 ve üzerinde yapılır. IP paketleri ve UDP paketleri kriptosuz gönderilir. Bu sayede Layer 3 ve 4 kapsamında Header Compression yapılabilir [6].

FNBDT/SCIP sinyalleşmesi esas olarak bağlantı kurma ve kontrol sinyalleşmelerinden oluşur. Bağlantı Kurma Sinyalleşmesi; Yetenekler, Parametre/Sertifika, F(R) (Forward and Reverse) ve Kripto Senkronizasyon (CryptoSync); Bağlantı Kontrol Sinyalleşmesi ise İhbar İşlemleri (Notification), Mod Değiştirme ve Senkronizasyonu Tekrar Kurma konularını içerir.



Şekil 1. FNBDT/SCIP protokol altyapısı [2] (FNBDT/SCIP protocol infrastructure)

FNBDT/SCIP sinyalleşmesi, Şekil 2'de görüldüğü gibi, sekiz baytlık SOM (Start of Message) ile başlayıp sekiz baytlık EOM (End of Message) ile sonlanır. SOM ve EOM arasında gönderilen çerçeveler "çerçeve grubu (super frame)" olarak tanımlanır. Her çerçeve grubu gönderme yönünde hata düzeltimi FEC (Forward Error Correction) ve çevrimsel artıklık denetimi CRC (Cyclic Redundancy Check) ile korunan çerçevelerden meydana gelmekte olup, FEC ile düzeltilemeyen hataların ortadan kaldırılması içinse olumlu veya olumsuz onay verme mekanizmaları (ACK ve NACK) kullanılır.



Şekil 2. FNBDT/SCIP çağrı kurma sinyalleşmesi (FNBDT/SCIP call setup signaling)

Her bir çerçeve, 1 çerçeve numarası, 13 mesaj, 4 FEC ve 2 CRC olmak üzere 20 bayttan oluşur. Bu çerçevelerden oluşan ve SOM ile başlayıp EOM ile sonlanan her çerçeve grubu en az 1 (bir) en çok 127 adet çerçeveden oluşur.

EOM alındığında öncelikle son alınan çerçevenin ESCAPE veya REPORT olup olmadığına bakılır, eğer değilse o ana kadar alınmış çerçeveler için rapor hazırlanır ve gönderilir. ESCAPE mesajı band genişliği kullanımı, REPORT mesajı ise gelen çerçevelerin hata oran onayları ile ilgili kavramlardır.

Benzer şekilde FNBDT/SCIP sinyalleşmesinde karşılaşılabilecek mesaj türlerinden diğer bir tanesi RESET mesajıdır ki bu mesaj gerekli durumlarda iletim katmanını yeniden senkron hale getirmek için kullanılır. RESET mesajı çerçeve numaralarını sıfırlar, bir SOM ve EOM arasında yalnızca bir RESET mesajı gönderilir.

FNBDT/SCIP sinyalleşmesinde, bağlantı kurma sinyalleşmesinin ilk adımı olarak terminaller birbirlerine Yetenekler Mesajını (Capabilities Message) gönderirler. Bu mesaj sayesinde terminaller birbirleriyle uyumlu olarak ne şekilde çalışabileceklerini (açık veya kapalı modlar) belirlerler. Güvenli modda haberleşme yapılacak ise uygun anahtar listesinin seçilmesi de bu sayede mümkün olur. Yetenekler

Mesajı gönderildiği anda ilk mesaj zamanlayıcısı başlamakta, bu zamanlayıcı karşı taraftan FNBDT/SCIP uyumlu mesaj gelmemesi halinde bağlantının zaman aşımına uğramasını temin eder. Zaman aşımı sonunda Boş Bağlantı haline dönülür.

İlk mesajlaşma sonunda eğer güvenli haberleşme kararı verildiyse FNBDT/SCIP bağlantısı kurulabilmesi maksadıyla trafik anahtarını oluşturabilmek için karşılıklı sertifikaların ve F(R)'ların değiş tokuş yapılması gerekir. Bunlardan sertifikanın gönderilmesi Parametre/Sertifika mesajı ile olur.

F(R) mesajı anahtar takımı ile ilgili bir takım bilgileri (anahtarın tip, uzunluğu vb.), F(R) uzunluğu ve F(R)'ın kendisini kapsayan bir mesajdır. F(R) mesajı iletilmeden önce mutlaka parametre/sertifika mesajı iletilmiş olmalıdır.

FNBDT/SCIP bağlantısı kurmada diğer bir adım kripto senkronizasyon mesajlarının değişimidir. Değişimi yapılan sertifika ve F(R) bilgileri ile trafik anahtarı oluşturulur, bu anahtar ile test paketi şifrelenip Kripto Senkronizasyon Mesajı haline getirilir.

Bağlantı kurma sinyalleşmesinden sonra kurulan bağlantının değişikliklere tabi tutulmasıyla ilgili bir takım sinyalleşme tanımları mevcuttur. Bağlantı kontrol sinyalleşmesinin amacı; herhangi bir sebeple bağlantıyı sonlandırmak, mevcut uygulamayı değiştirmek, diğer terminali ikaz etmek ve/veya kripto senkronizasyonunu baştan sağlamak olabilir. Bağlantı kontrol sinyalleşmesinde dört farklı mesaj vardır. Bunlar; İhbar (Notification), Mod Değişim İsteği (Mode Change Request), Mod Değişim Yanıtı (Mode Change Response) ve Kripto Senkronizasyon'udur (Crypto Sync).

Mod değiştirme işlemi; talep ve buna verilen yanıt şeklinde iki türlüdür ve sadece her iki terminal de güvenli uygulama trafiğinde iken mümkün olabilir.

Güvenli Ses için beş farklı çağrı mevcuttur. Bunlar [7-8];

- Güvenli 2,4 kbps MELP kodlu Ses–Blank&Burst (DTX),
- Güvenli 2,4 kbps MELP kodlu Ses–Blank&Burst (FCT),
- Güvenli MELP kodlu Ses –Burst w/o Blank (DTX),
- Güvenli MELP kodlu Ses –Burst w/o Blank (FCT),
- Güvenli, Gelişmiş Çoklu-Band Uyarımı (AMBE)'dır.

FNBDT/SCIP'de Blank & Burst ve Burst w/o Blank olmak üzere iki tip güvenli ses çağrısı yapılabilmektedir.

FNBDT/SCIP uyumlu bir terminalde, kripto senkronizasyonunun sürekliliği için belirli periyotlarla terminal tarafından 2,4 kbps'de üretilen MELP kodlu ses bilgisinin üzerine kripto senkronizasyon bilgisi yazılır. Bu işleme "B&B" (Blank and Burst) protokolü denilir. Uygulamada, zaman zaman ses bilgisi silinerek, yerine kripto bilgisi yazılmasından dolayı ses kalitesinde ufak çapta düşüşler yaşanır.

Blank & Burst çerçeve grubu 24 çerçeveden oluşmasına karşın, Burst w/o Blank uygulaması 25 çerçeveden oluşur. Dolayısıyla Burst w/o Blank uygulaması için gerekli kanal kapasitesi 2,4 kbps'den fazla olur. Aynı zamanda, MELP kodlanmış ses bilgilerinin üzerine kripto senkronizasyon bilgisi yazılmadığı için ses kalitesi B&B'ye göre daha iyidir.

Açık MELP ses çağrı hizmeti görüşmesinde de ortaya çıkan yapı, tıpkı B&B'de olduğu gibidir. Mesaj yine, biri SM (Synchronization Management) çerçevesi olmak üzere toplam 24 çerçeveden oluşan çerçeve gruplarıyla yapılır. Ancak burada kriptolama yapılmadığından SM çerçevesinin başlık kısmından sonrası sıfır ile doldurularak mesaj gönderilir.

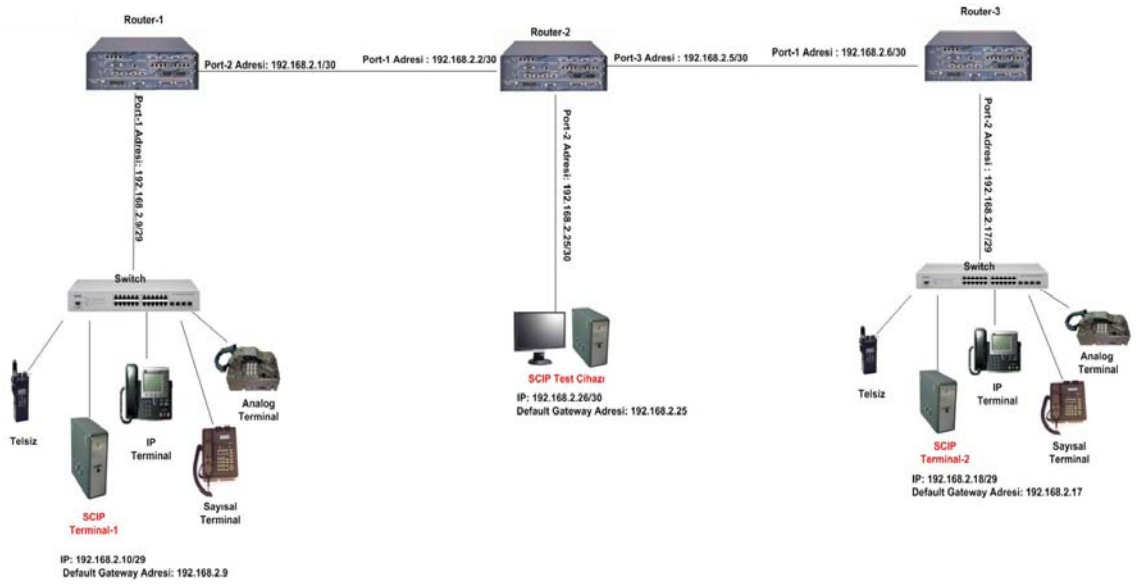
Ayrıca ister güvenli, isterse açık olarak görüşen tüm FNBDT/SCIP uyumlu terminallerin DTX ve FCT durumlarını desteklemesi beklenir. Burada, DTX; bir ses çağrısı sırasında, terminalin kullanıcısı konuştuğu sürece çerçeve gruplarının oluşturularak gönderilmesi, kullanıcı sustuğunda ise gönderme yapmanın kesilmesi prensibini, FCT ise; ses çağrısı sırasında terminalin kullanıcısının sustuğu sürede de çerçeve gruplarının oluşturularak karşı terminale iletilmesi, yani MELP kodlayıcı biriminin sürekli çalışmasını ifade etmektedir.

FNBDT/SCIP, veri haberleşmesinde ise iki veri hizmetini destekler. Bunlar "Güvenli Aktarım RT (Reliable Transport) Asenkron Veri Hizmeti" ve "Garanti İş GT (Guaranteed Throughput) Asenkron Veri Hizmetleridir.

RT Asenkron Veri hizmetinde, güvenli ses hizmetinde kullanılan sinyalizasyon mekanizmalarının aynısını kullanarak veri çağrısı başlatılır ve kanal kapasitesi %70 verimlilikle kullanılır. GT Asenkron Veri hizmeti ise kanal kapasitesinin tamamının kullanıldığı bir servistir [7-8].

3. UYGULAMA İÇİN KURULAN AĞ (NETWORK FOR APPLICATION)

FNBDT/SCIP protokolünün IP ağlar üzerindeki davranışını incelemek amacıyla Şekil 3'te verilen IP test düzeneği laboratuar ortamında kurulmuş, gerekli parametre değişiklikleri yapılıp, istenilen ölçümler yapılmıştır. Şekilde görüldüğü gibi test düzeneği;



Şekil 3. Üzerinde FNBDT/SCIP uygulamasının yapıldığı IP ağ (IP network on which FNBDT/SCIP application is executed)

- Çağrıyı başlatan FNBDT/SCIP Terminal,
- Haberleşme ortamını test eden FNBDT/SCIP Test Cihazı,
- Çağrıyı cevaplayan FNBDT/SCIP Terminal,
- Router-1, Router-2 ve Router-3 ile oluşturulmuş 3 adet yerel alan ağından (YAA)

oluşmaktadır.

Bu uygulamada FNBDT/SCIP Terminali olarak FNBDT/SCIP Emulator programı ve Haberleşme ortamını test etmek için FNBDT/SCIP Test Tool programı kullanılmıştır. FNBDT/SCIP Test Tool programı sayesinde farklı senaryolara göre, Bit Hata Oranı, Veri Kaybı ve Gecikme durumları oluşturulmuştur.

Uygulama esnasında ağ üzerinde FNBDT/SCIP uygulamasını etkileyecek yoğun bir trafik olmamıştır. Bu nedenle uygulama sırasında ağ üzerindeki trafik etkisini en aza indirgemek için Cisco'nun 3800 serisi Routerlar tercih edilmiş ve sisteme FNBDT/SCIP paketleri dışında hiçbir paket verilmemiştir.

Uygulamada geçen bazı önemli kavram ve tanımlar bölümünde verilmiştir.

4. UYGULAMA (APPLICATION)

Uygulama için Şekil 3'de resmedilen ağ yapısı kullanılmıştır. İcra edilen uygulamalar, IP Ağ altyapısında FNBDT/SCIP haberleşme davranışlarının değişik durumlar altında gözlenmesi maksadıyla yapılmıştır. Çalışma esnasında yapılan testler; tekrarlanmak suretiyle elde edilen verilerin ve test ortamının güvenilirliği, mümkün olduğunca uzun tutularak, verilerin geçerliliği sınanmıştır.

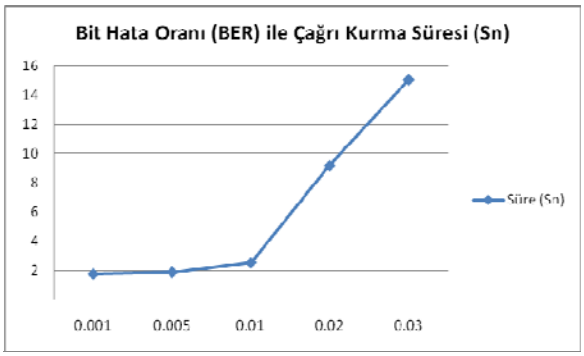
FNBDT/SCIP sinyalleşmesinin kritik evrelerini teşkil etmeleri nedeniyle çalışmada daha çok FNBDT/SCIP sinyalleşmesinin "Çağrı Kurma" ve "Güvenli Veri Aktarımı" bölümlerindeki denemeler yoğunluk kazanmıştır. Bununla beraber "Güvenli Ses Haberleşmesi" konusunda da çalışmalar yürütülmüş ve bir takım sonuçlara ulaşılmıştır.

Genel olarak çalışma, Çağrı kurma (Call Setup), B&B Güvenli Ses, B w/o B Güvenli Ses, RT Asenkron Güvenli Veri, GT Asenkron Güvenli Veri, olmak üzere beş ana başlık ve her ana başlığın altında Bit Hata Oranı ve Veri Kayıpları durumlarının değerlendirildiği iki alt başlık altında yapılmıştır.

4.1. Çağrı Kurma Uygulamaları (Call Setup Applications)

Normal Hallerde Çağrı Kurma:
FNBDT/SCIP Çağrı Kurma Sinyalleşmesi'nin ilk mesajı SOM ile başlamakta ve ses veya veri haberleşmesinin başlayabileceğine işaret eden START mesajı ile çağrı kurma sinyalleşmesi tamamlanmaktadır. Laboratuar ortamında yapılan deneysel testler sonucunda çağrı kurma işleminin ortalama 1,818 saniyelik bir zaman diliminde gerçekleştiği saptanmıştır. Bu sonuç sonraki aşamalarda alınan sonuçların değerlendirilmesinde bir karşılaştırma noktası olacağından önemlidir.

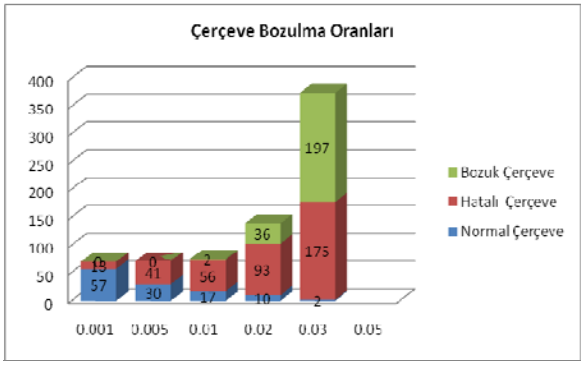
Bit Hata Oranı (BER) ile Çağrı Kurma:
Bu denemeler esnasında haberleşme ortamını test eden FNBDT/SCIP Test Cihazı tarafından iletişim kanalına belirli oranlarda bit hataları verilerek sonuçlar gözlenmiştir. Küçük bit hata oranlarından başlanarak hata oranları gittikçe artırılmış ve % 0.03'lük Bit Hata Oranına kadar FNBDT/SCIP bağlantı kurma işleminin mümkün olabileceği tespit edilmiştir (Şekil 4).



Şekil 4. BER (%) ile bağlantı kurma süresi grafiği (Diagram on connection setup duration with BER (%))

Şekil 4'deki grafikte görüldüğü gibi, Bit Hata Oranı arttırıldıkça, Çağrı Kurma Süresinin de arttığı, özellikle % 0.01 Bit Hata Oranından sonra bu artışın daha dikkat çekici bir değere ulaştığı gözlenmiştir.

Şekil 5'de, Bit Hata Oranı'nın çerçevelere etkisi görülmektedir. Bit Hata Oranı arttıkça, çerçevelerin neredeyse tamamının Hatalı ve Bozuk Çerçeve olarak iletildiği, toplam çerçeve sayısında ciddi artış olduğu gözlenmiştir. % 0.03 Bit Hata Oranında, hemen hemen tüm çerçevenin bozuk ve hatalı olduğu, çerçeve sayısında ise % 0.02 Bit Hata Oranına göre iki kattan fazla artış olduğu tespit edilmiştir.



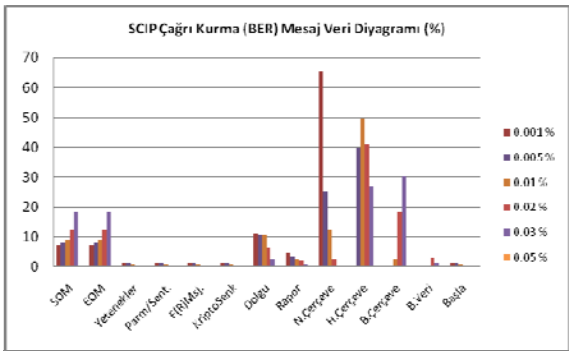
Şekil 5. Çerçeve bozulma oranları (Frame deterioration rates)

Burada; Hatalı Çerçeve, FEC ve CRC hata düzeltme algoritmalarıyla düzeltilmesi mümkün olan veri çerçevelerini, Bozuk Çerçeve ise, düzeltilmesi mümkün olmayan veri çerçevelerini ifade etmektedir.

Şekil 6, FNBDT/SCIP Çağrı Kurma esnasındaki verilerin % olarak değişimini göstermektedir. Şekilde görüldüğü gibi Bit Hata Oranı arttıkça Normal çerçeve sayı ve yüzdesinin azaldığı, diğer taraftan SOM, EOM, Hatalı ve Bozuk çerçeve miktarlarında artma olduğu tespit edilmiştir.

Veri Kaybı Durumlarında Çağrı Kurma:

Eksik Bit Oranı (Drop Bit Rate); Çalışmanın bu kısmında mesaj iletimi, FNBDT/SCIP Test Cihazı tarafından bit bazında veri kaybına uğratılarak, sonuçları değerlendirilmiştir. Tablo 1'de değişik Eksik Bit Oranları için mesaj miktarları ve bağlantı kurma süreleri verilmektedir.



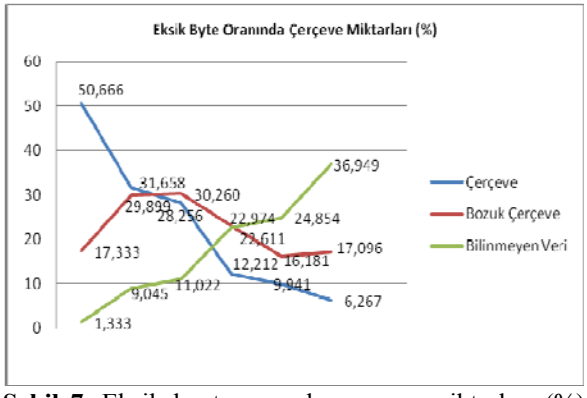
Şekil 6. BER ile çağrı kurma veri diyagramı (%) (Call setup (BER) message data diagram (%))

Tablo 1. Eksik bit oranı mesaj verileri (Drop bit rate message data)

Eksik Bit Oranı (%)	0,001	0,005	0,01	0,02
SOM	60	287	434	999
EOM	60	287	434	999
Hatalı Çerçeve	18	99	161	208
Çerçeve	127	169	98	66
Bozuk Çerçeve	122	370	572	1101
Yetenekler Msj.	1	1	1	1
Parm./Sert. Msj.	1	1	1	0
Rapor	4	3	4	3
F(R) Msj.	1	1	1	0
Kripto Senk.	1	1	1	0
Dolgu	12	11	11	11
BAŞLA	1	1	1	1
Bilinmeyen Veri	7	91	177	564
Topl. Mesaj	404	1331	1919	4022
Bağ Sür (sn)	12,078	37,453	67,453	125,860

Tablo 1'de de görüldüğü üzere FNBDT/SCIP bağlantı kurulması esnasında bit bazında veri kaybına uğratıldığında ciddi sorunlarla karşı karşıya kalınmış ve % 0,03 Bit Veri Kaybında bile çağrı kurulması mümkün olmamıştır.

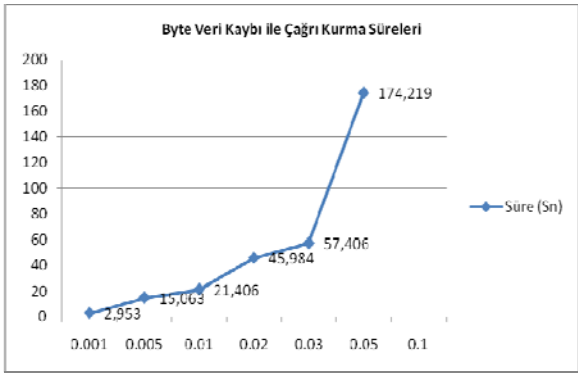
Eksik Bayt Oranı (Drop Byte Rate); Eksik Bit Oranı test sonuçlarının aksine bu kısımda yapılan denemelerde, veri iletimi esnasında Bayt tabanlı kayıpların yüksek kayıp oranlarına çıkılana kadar büyük problemlere yol açmadığı görülmüştür. Sadece dikkate değer değişiklik gösteren mesajların yer aldığı Şekil



Şekil 7. Eksik bayt oranında çerçeve miktarları (%) (Frame quantities in drop byte rate (%))

7'de, Normal Çerçevelerin, Eksik Bayt Oranları arttıkça azaldığı, buna karşın özellikle Bilinmeyen Verilerin ters orantılı olarak arttığı tespit edilmiştir.

% 0,05'lik bayt veri kaybının olduğu nokta FNBDT/SCIP çağrısının son olarak kurulabildiği değer olarak tespit edilmiştir. Bu noktada, Şekil 8'de görüldüğü gibi çağrı kurma süresi yaklaşık 174 saniyeye çıkarken iletilen verilerin % 36,949 (Şekil 7) sistem tarafından bilinmeyen veri olarak algılanmıştır.



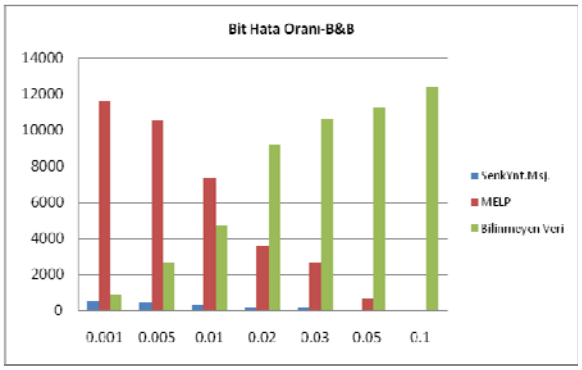
Şekil 8. Bayt veri kaybı (%) ile çağrı kurma süreleri (Call setup durations with drop byte rate (%))

4.2. Blank & Burst Güvenli Ses Haberleşmesi Uygulamaları (Blank & Burst Secure Voice Communication Applications)

Bu bölümdeki güvenli ses haberleşmesi, Blank & Burst (B&B) FCT (Force Continuous Transmission) olarak gerçekleştirilmiştir. Öncelikle FNBDT/SCIP çağrı kurma işlemi gerçekleştirilmiş ve çağrı kurma işleminden sonra farklı Bit Hata Oranı (BER), Eksik Veri (Bayt ve Bit) Oranı uygulanarak B&B Güvenli ses haberleşmesinde FNBDT/SCIP Test Cihazının imkanları dahilinde ölçümler yapılmıştır.

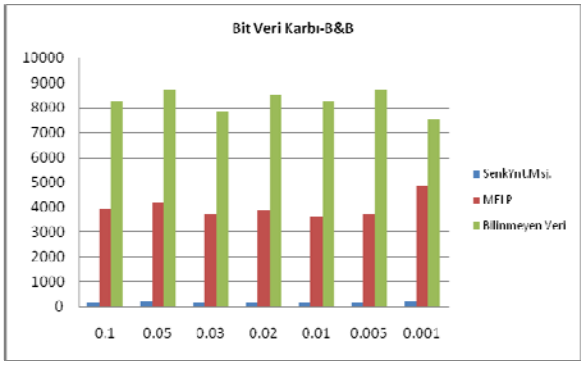
Bit Hata Oranı Etkileri:
Bu kısımda, FNBDT/SCIP çağrısı kurulduktan sonra sisteme belirli bit hata oranları sırasıyla verilerek B&B FCT ses haberleşmesi üzerinde oluşturduğu etkiler gözlenmiştir.

Şekil 9'da açıkça görüldüğü gibi, Bit Hata Oranı artıkça, Bilinmeyen Verinin artmasına karşılık MELP ve Senkronizasyon Yönetim Mesajı (Senk. Ynt. Msj.) azalmaktadır. Hatta Bit Hata Oranı % 0,1 olduğunda hemen hemen tüm verilerin bilinmeyen olduğu tespit edilmiştir.



Şekil 9. B&B ses görüşmesinde bit hata oranı (Bit error rate over B&B voice communication)

Veri Kaybı:
Şekil 10'da görüldüğü gibi Bit Veri Kaybının Ses görüşmesini etkilemediği, hata oranı ne olursa olsun görüşmenin devam ettiği tespit edilmiştir.



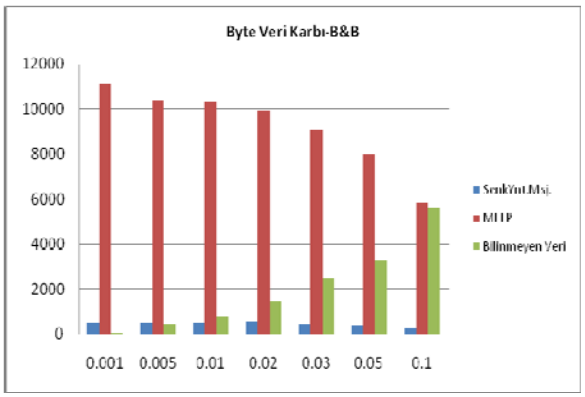
Şekil 10. Bit veri kaybında (%) B&B güvenli ses görüşmesi (B&B secure voice communication during drop bit rate (%))

Şekil 11'de sistem tarafından bayt veri kayıplarına verilen tepkiler görülmektedir. Bayt veri kayıplarında kritik eşik % 0,1 orandaki kayıplar olarak tespit edilmiştir.

4.3. Burst w/o Blank (B w/o B) Güvenli Ses Haberleşmesi Uygulamaları (Burst w/o Blank Secure Voice Communication Applications)

Bilindiği üzere B w/o B modunda MELP kodlu güvenli ses iletimi 24'lü MELP çerçeve grubuna ek 25'nci çerçeve olarak katılmaktadır. Bu sayede MELP çerçevelerinden biri eksilmediği için daha iyi ses kalitesine ulaşılabiliyorken, diğer yandan iletim hattında yarattığı ilave yük (overhead) ile daha yüksek band genişliklerine ihtiyaç duyulmasına sebep olmaktadır.

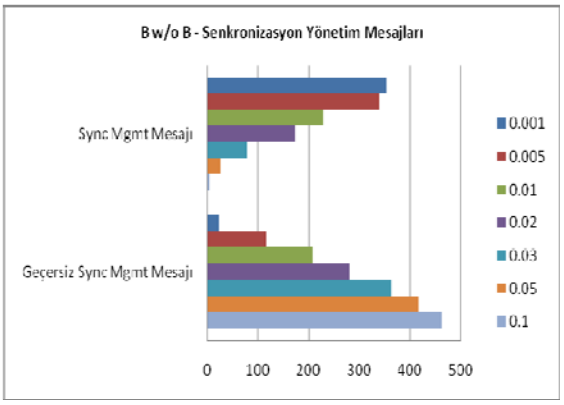
Testlerin bu bölümünde B w/o B güvenli ses



Şekil 11. Bayt veri kaybında (%) B&B güvenli ses görüşmesi (B&B secure voice communication during drop byte rate (%))

haberleşmesinin yukarıda belirtilen özelliğinden dolayı avantajlı bir durumun ortaya çıktığı tespit edilmiştir. Bu avantajlı durum, Bit Hata Oranı ve Eksik Veri (Bit ve Bayt) Oranı durumlarında ses görüşmesinin uzun süre sürdürülebilmesidir.

Bit Hata Oranı Etkileri:
Şekil 12'de görüldüğü üzere, Bit Hata Oranı arttıkça, Geçersiz Senkronizasyon Yönetim mesajlarının arttığı, Geçerli Senkronizasyon Yönetim mesajlarının ise azaldığı tespit edilmiştir.



Şekil 12. B w/o B senkronizasyon yönetim mesajları (B w/o B synchronization administration messages at different bit error rates)

Veri Kaybı:
Bayt veri kaybı testlerinde; Bayt Veri Kaybı arttırıldıkça Geçersiz Senkronizasyon Yönetim Mesajlarının arttığı ve Senkronizasyon Yönetim Mesajlarının ise azaldığı tespit edilmiştir.

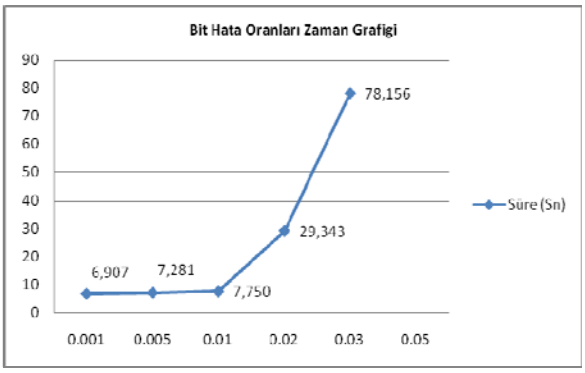
Bit veri kaybı testlerinde; Bit Veri Kaybı arttırılmasına rağmen Geçersiz Senkronizasyon Yönetim Mesajlarının ve Senkronizasyon Yönetim Mesajlarının sayısında ciddi bir değişiklik olmadığı tespit edilmiştir.

4.4. RT Asenkron Güvenli Veri Haberleşmesi (RT Asynchronous Secure Data Communication)

Bu tip güvenli veri iletiminde FNBDT/SCIP mesaj iletim mekanizması kullanılması dolayısıyla verilerin güvenli (Reliable) bir şekilde uzak uca ulaştırılması sağlanmış olur. Ayrıca bu iletim şeklinde Kripto Senkronizasyonu kayıpları olmadığından Senkronizasyon Yönetim Mesajı işlevleri görülmemektedir.

Bit Hata Oranı Etkileri:
Bit Hata Oranı ile RT Asenkron Güvenli Veri Aktarım testlerinde; öncelikle normal FNBDT/SCIP Çağrı Kurma işlemi yapılmış, sonra RT Asenkron Güvenli Veri Aktarım moduna geçilerek FNBDT/SCIP terminalleri arasında % 0,001 ile % 0,1, Bit Hata Oranları arasında deneme dosyasının aktarımı test edilmiştir.

Şekil 13, RT asenkron güvenli veri haberleşmesinde



Şekil 13. Farklı BER (%) değerlerinde veri aktarma (Data transfer at different bit error rates (%))

veri aktarma sürelerinin bit hata oranlarındaki değişimi göstermektedir.

Şekil 13'te görüldüğü gibi, zaman ekseninde ilk büyük artış % 0,01 bit hata oranından sonra gerçekleşmiştir. Bununla beraber, % 0,03 Bit Hata Oranının, RT Asenkron Güvenli Veri Aktarımı için son nokta olduğu tespit edilmiştir.

Veri Kayıpları
RT Asenkron Güvenli Veri Haberleşmesinde veri aktarmanın Bit Veri Kaybına karşı çok hassas olduğu tespit edilmiştir.

Eksik Bit Oranı Veri Kayıpları
% 0,001'lik bit kayıp oranında bile veri aktarım süresinin fazla olduğu tespit edilmiş olup bu bölümdeki çalışmalar % 0,01'lik Bit Veri Kaybına kadar yapılabilmiştir.

Eksik Bayt Oranlı Veri Kayıpları
Tablo 2'de, RT Asenkron Güvenli Veri Haberleşmesinde Bayt Veri Kaybı Etkileri ayrıntılı olarak verilmiştir. Verilen sonuçlardan anlaşılacağı üzere % 0,02 Eksik Bayt Oranının aşıldığı noktadan sonra veri aktarımı mümkün olmamıştır. (*) işaretli satırlar hata düzeltme mekanizmalarıyla düzeltilen mesajları göstermektedir.

Tablo 2. Bayt veri kaybı etkileri (Effects of drop byte rate)

Eksik Bit Oranı	0,001	0,005	0,01	0,02
SOM	203	787	1113	3474
SOM*	1	7	28	160
Çerçeve	1559	2421	2224	3705
Bozuk Çerçeve	423	1502	1953	4336
EOM	206	787	1113	3474
EOM*	1	7	28	160
Bilinmeyen Veri	43	460	820	4082
Süre (sn.)	30,438	72,765	95,296	258,25

4.5. GT Asenkron Güvenli Veri Haberleşmesi (GT Asynchronous Secure Data Communication)

GT Asenkron Veri Haberleşmesinde 2,4 kb/s veri aktarım hızı garanti edildiğinden FNBDT/SCIP Terminalleri arasında veri iletiminin daha hızlı olacağı

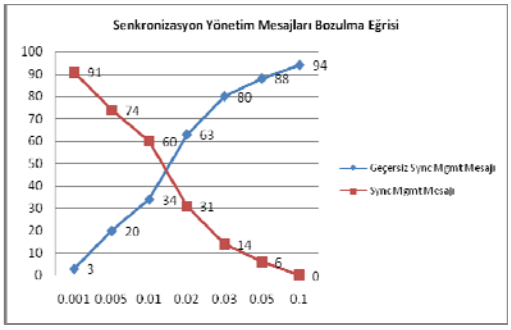
öngörülmektedir. GT Asenkron Veri Haberleşmesi, B w/o B Güvenli Ses Haberleşmesinde olduğu gibi tam bant olduğundan Senkronizasyon Yönetim Mesajları kullanılırken 24 adet olan MELP mesajlarından birinin kullanılması söz konusu değildir.

Tablo 3'de de görüldüğü gibi, gerçekten de normal (Bit Hata Oranının olmadığı) şartlarda yapılan denemelerden elde edilen sonuçlar aynı büyüklükteki verinin aktarım süresinin daha kısa olduğunu göstermektedir. RT Asenkron veri Aktarımında 6,698 saniye olan iletim süresi GT Asenkron veri Aktarımında 2,310 saniye olarak tespit edilmiştir.

Tablo 3. Veri aktarım sürelerinin karşılaştırması (Comparison of data transfer durations)

Bit Hata Oranı (%)	Süre (Sn)	
	GT	RT
0 (Hatasız)	2,310	6,689
0,001	3,900	6,907
0,005	3,954	7,281
0,01	4,070	7,750
0,02	3,793	29,343
0,03	3,867	78,156
0,05	4,026	Başarısız
0,1	4,800	Başarısız

Şekil 14'de görüldüğü gibi, Bit Hata Oranının Geçersiz Senkronizasyon Yönetim Mesaj oranıyla doğru, Senkronizasyon Yönetim Mesaj oranıyla ise ters orantılı olarak artığı tespit edilmiştir. Geçerli ve Geçersiz Senkronizasyon Yönetim Mesaj sayıları toplamının her Bit Hata Oranında aynı olup toplam mesajların % 6,6'sını oluşturduğu tespit edilmiştir.



Şekil 14. Senkronizasyon mesajlarının bozulması (Corruption of synchronization messages)

5. SONUÇLAR (CONCLUSIONS)

Bu çalışma, farklı şebekelerde haberleşme yapan cihazların birbirleri ile emniyetli haberleşme yapabilmesini amaçlamıştır. Uygulama olarak FNBDT/SCIP terminal emulatörleri vasıtasıyla IP ağı üzerinde yapılan test sonuçları sunulmuştur. Yakın gelecekte standartlaştırılması beklenen FNBDT/SCIP protokolünün gelişimine katkıda bulunmak ve ayrıca çalışma, özellikleri, içeriği bakımından konuyla ilgili yapılan ilk çalışmalardan birisi olması ve elde edilen test verilerinin müteakip çalışmalara girdi oluşturma olanakları sunması nedeniyle önemlidir.

Bu çalışma sonunda tespit edilen genel sonuçlar, olabilecek çözümler ve gelecekte yapılabilecek testler şu şekilde özetlenebilir:

1. FNBDT/SCIP çağrı kurmada, Bit Hata Oranının (BER), Bit ve Bayt Veri Kayıplarının her birinin farklı davranışlar sergilediği gözlenmiştir. Bit Hata Oranında sınır değer % 0,03, Eksik Bit Oranında sınır değer % 0,02 ve Eksik Bayt Oranında sınır değer ise % 0,05 olarak bulunmuştur.
2. FNBDT/SCIP bağlantısı kurulumunun Bit Veri Kaybına karşı çok duyarlı olduğu tespit edilmiştir.
3. Güvenli ses haberleşmesinin her iki (B&B ile B w/o B Güvenli Ses Haberleşme) şeklinde de diğer haberleşme modlarından farklı tepkiler alınmış, Bit Hata Oranlarının etkileri gözlenirken Veri Kayıplarının genelde önem arz etmediği tespit edilmiştir.
4. Bit ve Bayt Veri kayıplarının her iki türünde de RT Asenkron Güvenli Veri iletimini ciddi anlamda etkilediği belirlenmiştir.
5. GT Asenkron Veri Haberleşmesi ile ilgili testlerde Bit ve Bayt Veri Kayıplarının Garantili Veri İletimini olumsuz olarak etkilediği gözlenmiştir.
6. FNBDT/SCIP sinyalleşmesi için haberleşme modu her ne olursa olsun % 0,03'lük Bit Hata Oranının sınır değer olarak genel kabul görür bir nokta olduğu anlaşılmıştır. Saptanan bu sonucun, denemenin yapıldığı IP ortamında yüksek bir oran olarak ortaya çıktığı gözlenmiştir.
7. BER arttıkça çağrı kurma süresi artmakta ve normal çerçeve sayısı azalmaktadır. Normal çerçevelerin yerini hatalı ve bozuk çerçeveler almaktadır ve çerçeve miktarının genelinde bir artış olmaktadır. Çerçeve miktarının genelindeki artış SOM ve EOM mesajlarının artmasına neden olmaktadır. Bu yüzden de çağrı kurulum süresi artmaktadır. BER'in arttırılmasına rağmen toplam çerçeve sayısı sabit tutulabilinirse SOM ve EOM paketlerinin sayısı sabit tutulmuş olunur ve çağrı kurulum süresi belli bir BER değerine kadar artmaz, sabit kalır.
8. FNBDT/SCIP uygulamalarındaki kriptolama işlemi uygulama katmanında yapıldığı için alt katmanlarda Header Compression teknikleri uygulanarak daha az bir bant genişliği tahsisi ile çağrı kurulumuna olanak sağlanabilinir.

ÖNEMLİ KAVRAM VE TANIMLAR (IMPORTANT CONCEPTS AND DEFINITIONS)

FNBDT/SCIP Emulatör: Laboratuvar ortamlarında cihazların karşılıklı çalışabilirliğini değişik senaryolar ve durumlar dahilinde test eden bir yazılım uygulamasıdır.

FNBDT/SCIP Tester: FNBDT/SCIP Emülatör Yazılımının bir parçası olup, terminaller arası

FNBDT/SCIP haberleşmesinin takip ve kontrol edilmesi maksadıyla kullanılır. Modülün içerisinde sürece etki edilebilmesini (bozma, karıştırma, geciktirme vb.) sağlayan fonksiyonlar mevcuttur.

Bit Hata Oranı (Bit Error Rate-BER): Belli bir zaman aralığında iletilen veri bitlerinden hatalı olanların, aktarılan toplam bit sayısına oranı olarak tanımlanır.

Veri Kaybı (Data Loss): Bit veya Bayt olarak hatalı aktarılan veri miktarının toplamda aktarılan veriye oranıdır. Uygulamada kanal simülatörü tarafından yaratılan bu durumda bit kayıpları için bitler, bayt kayıpları içinse sekizli bit gruplarının rastlantısal olarak iletilmesi engellenerek veri kaybına yol açılır.

Gecikme (Delay): Aktarılan veride oluşturulan sistematik zaman kaymaları bu başlık altında tanımlanmaktadır.

KAYNAKLAR (REFERENCES)

1. Supplee, L., Cohn, R., ve Collura, J., "MELP: The New Federal Standard at 2400bps", **IEEE International Conference on Acoustic, Speech, and Signal Processing ICASSP'97**, Cilt.2, Sayfa 1591-4,1997.
2. Daniel, E.J. ve Teague, K.A., "Performance of FNBDT and Low Rate Voice (MELP) Over Packet Networks," **Proc.35th Asilomar Conference on Signals, Systems, and Computers**, Pacific Grove, California, Cilt.2, 1568-1572, 2001.
3. A.McCree and T. Barnwell, "A Mixed Excitation LPC Vocoder Model for Low Bit Rate Speech Coding", **IEEE Transaction of Acoustics, Speech, and Signal Processing**, Vol.3, No.4, pp.242-50, July 1995.
4. McCree, A.V. ve Barnwell, T.P., "A 2400 bps Mixed Excitation LPC Vocoder model for low bit rate speech coding", **IEEE Transactions on Speech and Audio Processing, Cilt**. 3, 242-250, 1995.
5. Dilli, O., Mert, M., Koyuncu, M., Nazlıbilek, S.ve Akçam, N., "SCIP (Secure Communication Interoperability Protocol)'in IP Ağları Üzerinde Uygulaması", **3. Bilgi Güvenliği ve Kriptoloji Konferansı**, ISC TURKEY, Ankara, Aralık 2008.
6. Daniel, E.J., Teague, K.A., Sleezer, R., Brewer, J., Raymond, J., Beck, W.J., Hershberger, J., "The Future Narrowband Digital Terminal**," IEEE**, pp. II-589-591, Stillwater, OK, 2002.
7. Bozoklu, O., **Uyumlu ve Birlikte Çalışabilir Güvenli Muhabere Kapsamında NATO/SCIP Bünyesindeki Kripto Standartlarına Türkiye'nin Yaklaşımı**, Yüksek Lisans Tezi, Kara Harp Okulu, Savunma Bilimleri Enstitüsü, 2007.
8. Ören, Ö., **Geleceğin Darband Sayısal Terminali**, Yüksek Lisans Tezi, Sakarya Üniversitesi, Fen Bilimleri Enstitüsü, 2005.